日　本　国　特　許　庁
JAPAN　PATENT　OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:　２００２年　７月１５日

出願番号
Application Number:　特願２００２－２０５０７２

[ST.10/C]:　[ＪＰ２００２－２０５０７２]

出願人
Applicant(s):　株式会社日立製作所

２００３年　５月１３日

特許庁長官
Commissioner,
Japan Patent Office　太田信一郎

出証番号　出証特２００３－３０３５５６４

【書類名】　特許願
【整理番号】　K02005601
【提出日】　平成14年 7月15日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 15/00　330
【発明者】
【住所又は居所】　神奈川県海老名市下今泉８１０番地　株式会社日立製作所　インターネットプラットフォーム事業部内
【氏名】　幕田　好久
【特許出願人】
【識別番号】　000005108
【氏名又は名称】　株式会社日立製作所
【代理人】
【識別番号】　100080001
【弁理士】
【氏名又は名称】　筒井　大和
【電話番号】　03-3366-0787
【手数料の表示】
【予納台帳番号】　006909
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報ネットワークシステムの制御方法および情報ネットワークシステムならびに移動通信端末

【特許請求の範囲】

【請求項１】　有線または無線の情報ネットワークに複数の情報処理装置を接続した構成の情報ネットワークシステムの制御方法であって、

個々の前記情報処理装置の前記情報ネットワークに対する接続位置に関する第１位置情報と、当該情報処理装置の現在位置を示す第２位置情報とを用いて、当該情報処理装置の前記情報ネットワーク上における情報資源へのアクセスの可否を制御することを特徴とする情報ネットワークシステムの制御方法。

【請求項２】　有線または無線の情報ネットワークと、前記情報ネットワークに接続され、当該情報ネットワーク上の情報資源にアクセスする第１情報処理装置と、前記第１情報処理装置の前記情報ネットワークに対する接続位置に関する第１位置情報および当該第１情報処理装置の現在位置を示す第２位置情報を用いて、前記第１情報処理装置の前記情報資源へのアクセスの可否を制御する第２情報処理装置と、を含むことを特徴とする情報ネットワークシステム。

【請求項３】　有線または無線の情報ネットワークに接続される移動通信端末であって、前記情報ネットワークに接続するための第１通信手段と、当該移動通信端末の現在位置の取得に用いることが可能な第２通信手段と、前記現在位置情報を前記情報ネットワークに送出する機能とを含むことを特徴とする移動通信端末。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報ネットワーク技術および移動通信端末に関し、特に、共有可能なファイル等の情報資源を持つ複数の端末とファイルサーバが有線または無線でネットワーク接続された環境において、認証サーバがおのおのの端末とファイルサーバの位置情報を元にファイルの共有制御をする認証技術に関する。

【０００２】

【従来の技術】

端末やファイルサーバは、情報の共有を実現するためにネットワークを通じて接続されている。無線ネットワーク接続においては、端末やファイルサーバは無線ＬＡＮのアクセスポイントを通じて無線電波で通信を確立できる。

【０００３】

しかし、その無線電波の到達範囲は不定であり、無線電波到達範囲内に存在する想定外の端末がネットワークに接続し、悪意ある使用者がその端末を操作して証拠を残さずに、別な端末やファイルサーバから情報を入手できる可能性がある。

【０００４】

【発明が解決しようとする課題】

上記従来技術では、無線通信の可能な範囲が限定されないため、無線電波到達範囲内に存在する想定外の端末がネットワークに接続された場合について配慮がされておらず、情報漏洩を引き起こす懸念がある、という技術的課題があった。

【０００５】

なお、特開２０００－２１５１６９号公報には、無線端末のＬＡＮへのアクセスポイント毎に特定データセットを割り当てることにより、アクセスポイントが変化する毎に当該特定データセットへのアクセスが自動的に行われるようにした技術が開示されているが、当該無線端末の位置を識別するために用いられる位置情報はアクセスポイントの位置情報のみであるため、たとえば建物内の各部屋毎にアクセスポイントを割り当てて各部屋を移動する毎にアクセス可能なデータセットを切り替えることはできるものの、建物の外からのアクセスが識別できず、情報漏洩等の上述の技術的課題は依然として解決されない。

【０００６】

本発明は、通信の可能な範囲を限定し、想定外の端末からのネットワーク接続を拒否することを目的としており、限定された範囲内でのみのネットワーク接続環境を提供し、情報漏洩やなりすましを防ぎ的確な情報伝達を可能とすることを目的とする。

【０００７】

また、本発明は、各端末およびファイルサーバにおいて、自身と複数のＧＰＳ衛星または複数の携帯電話基地局との間の距離から、自身の位置情報を取得することを目的とする。

【０００８】

さらに、本発明は、認証サーバにおいて、各端末およびファイルサーバから受信した位置情報から、各端末及びファイルサーバの通信可能な範囲の決定と通信範囲の制御を行なうことを目的とする。

【０００９】

【課題を解決するための手段】

本発明は、有線または無線の情報ネットワークに複数の情報処理装置を接続した構成の情報ネットワークシステムの制御方法であって、個々の情報処理装置の情報ネットワークに対する接続位置に関する第１位置情報と、当該情報処理装置の現在位置を示す第２位置情報とを用いて、当該情報処理装置の情報ネットワーク上における情報資源へのアクセスの可否を制御するものである。

【００１０】

より具体的には、一例として、有線、あるいは無線でネットワーク接続された端末やファイルサーバの現在位置情報（第２位置情報）を取得し、認証サーバにおいてそれぞれの現在位置情報と、アクセスポイント（ネットワークセグメント）の位置情報（第１位置情報）に基づいて、それぞれの通信可能範囲の設定を行ない、それぞれが限定された範囲内にある端末やファイルサーバとのみ情報の送受信を行なう。

【００１１】

また、上記構成において、端末やファイルサーバの位置情報は、それ自身と複数台のＧＰＳ衛星との距離から得た情報を元に取得する。もしくは、端末やファイルサーバの位置情報は、それ自身と複数台の携帯電話基地局との距離から得た情報を元に取得する。もしくは、端末やファイルサーバの位置情報は、それ自身とその端末やファイルサーバが接続可能な無線ＬＡＮアクセスポイントの位置情報を元に取得する。

【００１２】

そして、上記構成において、認証サーバは、各端末およびファイルサーバから受信した位置情報から、各端末及びファイルサーバの通信可能な範囲の決定と通信範囲の制御を行なう。

【００１３】

端末またはファイルサーバは、認証サーバ経由で他の端末またはファイルサーバからファイルを取り出すことができる。

【００１４】

ある端末に対するアクセス要求がその端末の通信可能範囲から逸脱していた場合、認証サーバはその端末に対するアクセスを認めないことでアクセス制御を行なう。

【００１５】

【発明の実施の形態】

以下、本発明の実施の形態を図面を参照しながら詳細に説明する。

【００１６】

図１は、本発明の一実施の形態である情報ネットワークシステムの制御方法を実施する情報ネットワークシステムの構成の一例を示す概念図である。

【００１７】

本実施の形態では、情報ネットワークの一例として、各端末がそれぞれにＧＰＳ（Global Positioning System ）等によって位置情報を得て、認証サーバにおいて共有する端末決定するネットワークシステムを例に採って説明を進める。

【００１８】

本実施の形態のネットワークシステムは、図１に示すように、共有可能なファイルを持つ自由に移動可能な複数の端末３００，３０１，３１１～３１５（以下、端末３ｘｘと総称する）と、共有可能なファイルを持つ特定位置に固定されたファイルサーバ４１１～４１３（以下、４１ｘと総称する）と、端末３ｘｘの位置情報を収集し各端末のアクセス許可範囲を決定しアクセス制御を行なう認証サーバ４００と、各端末３ｘｘが認証サーバ４００に接続するために設置する無線ＬＡＮアクセスポイント１０１と、端末３ｘｘの位置情報を得るのに使用する複数のＧＰＳ衛星５０１，５０２，５０３（以下、５０ｘと総称する）と、から成

る。

【００１９】

端末３ｘｘの各々は、無線ＬＡＮアクセスポイントとの間における無線通信を行うための無線ＬＡＮアクセス機能３００ａと、ＧＰＳ衛星５０ｘとの通信にて当該端末３ｘｘの現在位置情報を得るＧＰＳ受信機能３００ｂと、この現在位置情報を無線ＬＡＮ上に送出する機能とを備えている。

【００２０】

また、ファイルサーバ４１ｘの各々も自身の位置情報を取得して認証サーバ４００に送出する機能を備えることができる。

【００２１】

なお、端末３ｘｘが携帯電話機能を含む場合には、ＧＰＳ受信機能３００ｂとしては、公衆携帯電話網の図示しない基地局との位置関係から現在位置を取得する機能が実装される。

【００２２】

図２は、共有可能なファイルを持つ端末、ファイルサーバがどの領域にある端末に対してアクセスを認めるか否かを制御する認証処理に用いられる情報テーブルの構成の一例を示す概念図である。

【００２３】

本実施の形態の情報テーブル６００は、無線ＬＡＮアクセスポイント６００ａの各々毎に、アクセス許可領域６００ｂ、許可範囲（ｘ，ｙ）座標からなる受信許可範囲６００ｃ、アクセス先端末リスト６００ｄ、アクセス元端末リスト６００ｅの各情報が対応付けて格納されている。なお、無線ＬＡＮアクセスポイント６００ａ、アクセス許可領域６００ｂ、アクセス先端末リスト６００ｄ、アクセス元端末リスト６００ｅの各数値は、図１の各部の符号を示している。

【００２４】

また、受信許可範囲６００ｃの許可範囲（ｘ，ｙ）座標の数値は、簡単のため簡略な数値が設定されているが、実際には、たとえば、各端末の現在位置（経度，緯度等）に基づく認証の基準値が設定されている。

【００２５】

共有可能なファイルを持つファイルサーバ４１１は、アクセス許可領域として領域２１１が設定されていて、情報テーブル６００に保存されている。

【００２６】

領域２１１内にある端末３１１は、無線ＬＡＮアクセスポイント１０１と通信が可能であり、かつＧＰＳ衛星５０ｘから情報の取得が可能である。

【００２７】

端末３１１は、ＧＰＳ衛星５０ｘより情報を取得し、その情報を元に自身の位置情報を算出する。

【００２８】

端末３１１は、自身の位置情報を無線ＬＡＮアクセスポイント１０１を経由して認証サーバ４００に送信する。

【００２９】

また端末３１１は、認証サーバ４００から自身の位置情報の送信要求があった場合、速やかに自身の現在の位置情報を返信する。

【００３０】

なお、この端末からの現在位置情報の送信方法としては、標準の無線ＬＡＮプロトコルの接続開始時等の情報フレームにおけるベンダユニークな領域を使用することが考えられる。そして、認証サーバでは、当該ベンダユニークな領域に所定のフォーマットにて位置情報が設定されている場合には、送信元の当該端末が本実施の形態の認証技術に対応した機能を持つものとして、ファイルサーバへのアクセス許可等の後述の認証処理を実行し、設定されていない場合には、一般の端末として、最もセキュリティレベルの低い一般公開用データのみにアクセスさせる等の処理を行うことができる。

【００３１】

これにより、既存の無線ＬＡＮプロトコルの汎用性を損なうことなく、本実施の形態の認証機能を実装することができる。

【００３２】

このような端末３ｘｘの動作の一例を図７のフローチャートに例示する。

【００３３】

すなわち、まず、ＧＰＳ等から自身の現在位置情報を取得する動作（ステップ９２１）を、最寄りの無線ＬＡＮアクセスポイントの通信可能領域に入るまで繰り返し（ステップ９２２）、通信可能領域に入ったら、認証サーバ４００に現在位置情報および接続中の無線ＬＡＮアクセスポイント（ネットワークセグメント）の位置情報を、無線ＬＡＮアクセスポイントを経由して送信してアクセス要求を行う（ステップ９２３）。

【００３４】

そして、認証サーバ４００からのアクセス許可信号を待ち（ステップ９２４）、アクセス許可の場合には（ステップ９２５）、ファイルサーバへのアクセス要求を行い（ステップ９２６）、データを取得する（ステップ９２７）。また、アクセス不許可の場合には、ファイルサーバへのアクセスを行わない（ステップ９２８）。

【００３５】

認証サーバ４００は、受信した端末３１１の位置情報が、図２の情報テーブル６００のアクセス許可範囲内に収まっている場合、アクセス元端末リスト６００ｅに端末３１１を加える。

【００３６】

また、アクセス元端末リスト６００ｅに登録された端末に対して、その端末の位置情報を定間隔で要求し、受信した端末の位置情報が情報テーブル６００のアクセス許可範囲から外れた場合や、位置情報の返信が無い場合は、アクセス元端末リスト６００ｅから端末情報を削除する。

【００３７】

ここで、端末３１１がファイルサーバから情報を取得しようとするとき、自身がいる領域２１１がアクセスを許可している端末について認証サーバ４００に問い合わせをする。

【００３８】

認証サーバ４００は、情報テーブル６００を参照し、領域２１１に対応する行６０１が指し示すアクセス元端末リスト６００ｅに端末３１１の情報があるので、端末３１１に対して、領域２１１に対応するアクセス先端末リスト６００ｄに

登録されているファイルサーバ４１１に対するアクセスを許可する。

【００３９】

情報テーブル６００を参照した結果、領域２１１に対応する行６０１が指し示すアクセス元端末に端末３１１の情報が無ければ、端末３１１はすでに領域２１１外に出たものとみなし、アクセスを認めない。

【００４０】

これにより、端末３１１は領域２１１にいる限り、無線ＬＡＮアクセスポイント１０１、ネットワークを経由してファイルサーバ４１１から情報を取得できる。

【００４１】

他の端末についても同様である。

【００４２】

領域２１２内にある端末３１２は、ファイルサーバ４１２にアクセス可能である。

【００４３】

領域２１３内にある端末３１３，３１４は、ファイルサーバ４１３と端末３００にアクセス可能である。

【００４４】

また、別な無線ＬＡＮアクセスポイント１０２からネットワーク接続している、領域２１４内の端末３１５は、端末３１２と端末３０１にアクセス可能であるが、端末３０１がネットワークに接続されていないので、端末３１２にのみアクセス可能である。

【００４５】

領域２００にある端末３０１は、どの無線ＬＡＮアクセスポイントとも通信が可能でないため、認証サーバ４００に接続することができない。無線ＬＡＮアクセスポイント１０１または１０２の通信可能範囲に入ると初めて認証サーバへの接続に成功し、領域のアクセス設定に従い通信が可能となる。

【００４６】

上述のような認証サーバの動作の一例を図６のフローチャートを参照して説明

する。

【００４７】

任意の端末３ｘｘが任意の無線ＬＡＮアクセスポイントの通信可能範囲内にあるかを監視し（ステップ９１１）、通信可能範囲内にある場合には、当該端末から当該端末の現在位置情報を取得し（ステップ９１２）、当該端末の現在位置が個々の無線ＬＡＮアクセスポイント毎に設定された受信許可範囲内にあるかを調べ（ステップ９１３）、受信許可範囲内にある場合には、当該端末にアクセス許可信号を送信し（ステップ９１４）、情報テーブル６００のアクセス元端末リストに追加する（ステップ９１５）。

【００４８】

ステップ９１３で範囲外の場合には、当該端末にアクセス不許可を通知し（ステップ９１６）、アクセス元端末リストから当該端末を削除する（ステップ９１７）。

【００４９】

同様に、図５にて、ファイルサーバの動作の一例を説明する。

【００５０】

任意の端末からのアクセス要求を監視し（ステップ９０１）、要求がない場合には当該端末との送受信を停止する（ステップ９０２）。

【００５１】

アクセス要求がある場合には自ファイルサーバのマルチメディア情報等の情報配信サービス等に対応した端末か否かを判別し（ステップ９０３）、未対応の場合にはサービス案内を通知する（ステップ９０４）。

【００５２】

サービス対応の端末の場合には、さらに、アクセス元端末リストに当該端末が登録されているか調べ（ステップ９０５）、登録済み（すなわち、認証済み）の場合には、当該端末との送受信を確立する（ステップ９０７）。未登録の場合には、当該端末にアクセス不可メッセージを送信する（ステップ９０６）。

【００５３】

ところで、もし、無線ＬＡＮアクセスポイント１０１と１０２が同じビル内の

異なる階をカバーする領域を持つ場合、ＧＰＳ衛星から得た位置情報のみではその端末がどの階にあるのか、認証サーバ４００は把握できない。この技術的課題の解消のために、本実施の形態では、その端末が使用している無線ＬＡＮアクセスポイント（ネットワークセグメント）も記録しておき、端末の現在位置と併用して認証に用いることで、高さ方向の違いも考慮可能である。これは、無線ＬＡＮで使用する電波がビルの壁を通り抜けないことを利用している。

【００５４】

すなわち、図３に例示されるように、二階建ての建物７００の一階フロア２１１ａ（１Ｆ）、二階フロア２１４ａ（２Ｆ）の各々に無線ＬＡＮアクセスポイント１０１，１０２を設置し、無線ＬＡＮアクセスポイント１０１に対する端末のアクセス許可領域として領域２１１を一階フロア２１１ａの床範囲に設定し、同様に無線ＬＡＮアクセスポイント１０２に対する端末のアクセス許可領域として領域２１４を二階フロア２１４ａの床範囲に設定しておく。そして、認証サーバ４００では、個々の端末３１１，３１５の現在位置情報の他に無線ＬＡＮアクセスポイント１０１，１０２の位置情報を、ファイルサーバ４１ｘ等の持つデータへのアクセスの可否を決定する認証に用いることで、各階毎に当該階内に位置する個々の端末３１１，３１５を正確に識別でき、的確なデータアクセス制御が可能になる。

【００５５】

この方法による利点は、無線ＬＡＮアクセスポイント１０１，１０２の通信可能領域２０１，２０２の範囲内であっても、特定範囲の外にある端末とファイルの共有をするための通信を遮断することができ、また端末側にこのシステムに対する特殊な機構を用意する必要が無い。不正な端末を排除する目的での使用を想定できる。

【００５６】

すなわち、たとえ、建物７００からの無線ＬＡＮの電波漏洩があって、建物７００の外部に位置する端末が無線ＬＡＮに接続できたとしても、その端末の現在位置情報がアクセス許可領域の外であると判定できるため、認証不可と判定することができ、データアクセスのセキュリティを維持できる。

【００５７】

上述の本実施の形態の認証方法を応用することで、例えば図４のようなＣＤショップの運営に適用できる。

【００５８】

ＣＤショップ８００内は各ジャンルごとに領域が決められていて、領域２１はロックのＣＤが陳列してある場所、領域２２はジャズＣＤが陳列してある場所とする。それぞれの領域に対応した試聴用の音楽ファイルがファイルサーバ４１に格納されている。また、認証サーバ４０により、領域２１および領域２２は、それぞれロック音楽、ジャズ音楽の試聴データに対応付けられている。

【００５９】

ＣＤショップを通信可能範囲２０内に含む無線ＬＡＮアクセスポイント１に対する無線ＬＡＮアクセス機能３ａとＧＰＳ衛星５０ｘからのＧＰＳ受信機能３ｂを備えた携帯電話３を持った客がＣＤショップ内を歩いていて、領域２１内で携帯電話３を操作して試聴をしようとすると、認証サーバ４０が携帯電話３の現在位置情報に基づいてロック音楽の試聴データを当該携帯電話３に送信することでロック音楽の試聴データが携帯電話３の画面に表示され、そのデータを試聴できる。

【００６０】

同様にして、領域２１を外れ領域２２に移動すると、ロック音楽の試聴はできなくなり、代わりにジャズ音楽の試聴ができるようになる。

【００６１】

また、領域２１および領域２２が同一建物内の別階フロアの場合には、無線ＬＡＮアクセスポイントの位置情報を併用することで同様の切り替えや認証が可能なことは上述のとおりである。

【００６２】

この方法により、特定範囲に位置する携帯電話３にだけ試聴データを提供し、また以降の試聴データの不正使用も防ぐことができる。

【００６３】

他にも、オフィスにおいて外部に社内の情報が漏れないようにする手段など、

さまざまな応用方法が考えられる。

【００６４】

以上説明したように、本実施の形態によれば、共有可能なファイルを持つ複数の端末３ｘｘやファイルサーバ４１ｘが、有線または無線でネットワーク接続された環境において、認証サーバ４００が各々の端末とファイルサーバ４１ｘの位置情報を元にファイルの共有制御をするので、ネットワーク上のファイルに対するアクセス制御が可能となり、不正アクセスや成りすましの防止に効果がある。

【００６５】

さらに各端末３ｘｘおよびファイルサーバ４１ｘにおいて、自身と複数のＧＰＳ衛星５０ｘまたは複数の携帯電話基地局との間の距離から、自身の位置情報を取得するが、端末３ｘｘとファイルサーバ４１ｘにＧＰＳ受信装置もしくは、携帯電話受信装置を装着するのみで、すでにＧＰＳ衛星や携帯電話基地局が整備されており、いま現在あるものより大きな投資をすることなく、不正アクセスや成りすましの防止を効果的に実現できる。

【００６６】

さらに、認証サーバ４００において、各端末３ｘｘおよびファイルサーバ４１ｘから受信した位置情報から、各端末及びファイルサーバの通信可能な範囲の決定と通信範囲の制御を行なうので、正しい位置情報に基づいたアクセスに対してのみ通信を許可できるので、不正アクセスや成りすましの防止に効果がある。

【００６７】

本願の特許請求の範囲に記載された発明を見方を変えて表現すれば以下の通りである。

【００６８】

（１）．共有可能なファイルを持つ複数の端末とファイルサーバが有線または無線でネットワーク接続された環境において、認証サーバがおのおのの端末とファイルサーバの位置情報を元にファイルの共有制御をすることを特徴とするファイルアクセスの認証方法。

【００６９】

（２）．項目（１）記載の各端末およびファイルサーバにおいて、自身と複数

のＧＰＳ衛星または複数の携帯電話基地局との間の距離から、自身の位置情報を取得することを特徴とする方法。

【００７０】

（３）．項目（１）記載の認証サーバにおいて、各端末およびファイルサーバから受信した位置情報から、各端末及びファイルサーバの通信可能な範囲の決定と通信範囲の制御を行なうこと特徴とする方法。

【００７１】

以上本発明者によってなされた発明を実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。

【００７２】

【発明の効果】

通信の可能な範囲を限定し、想定外の端末からのネットワーク接続を的確に拒否して、限定された範囲内でのみのネットワーク接続環境を提供し、情報漏洩やなりすましを防ぎ的確な情報伝達を可能とすることができる、という効果が得られる。

【００７３】

各端末およびファイルサーバにおいて、自身と複数のＧＰＳ衛星または複数の携帯電話基地局との間の距離から、自身の位置情報を取得してセキュリティ管理に適用することができる、という効果が得られる。

【００７４】

認証サーバにおいて、各端末およびファイルサーバから受信した位置情報から、各端末及びファイルサーバの通信可能な範囲の決定と通信範囲の制御を行なうことができる、という効果が得られる。

【図面の簡単な説明】

【図１】

本発明の一実施の形態である情報ネットワークシステムの制御方法を実施する情報ネットワークシステムの構成の一例を示す概念図である。

【図２】

本発明の一実施の形態である情報ネットワークシステムの制御方法において用いられる情報テーブルの一例を示す概念図である。

【図３】

本発明の一実施の形態である情報ネットワークシステムの制御方法を実施する情報ネットワークシステムの構成の変形例を示す概念図である。

【図４】

本発明の一実施の形態である情報ネットワークシステムの制御方法を実施する情報ネットワークシステムの構成の応用例を示す概念図である。

【図５】

本発明の一実施の形態である情報ネットワークシステムにおけるファイルサーバの動作の一例を説明するフローチャートである。

【図６】

本発明の一実施の形態である情報ネットワークシステムにおける認証サーバの動作の一例を説明するフローチャートである。

【図７】

本発明の一実施の形態である情報ネットワークシステムにおける端末の動作の一例を説明するフローチャートである。

【符号の説明】

１０１，１０２　無線ＬＡＮアクセスポイント

２００　無線ＬＡＮアクセスポイントとの通信ができない領域

２０１　無線ＬＡＮアクセスポイント１０１と通信可能な領域

２０２　無線ＬＡＮアクセスポイント１０２と通信可能な領域

２１１～２１４　アクセス許可領域

３００，３０１，３１１～３１５　自由に移動可能な端末（第１情報処理装置）

３００ａ　無線ＬＡＮアクセス機能（第１通信手段）

３００ｂ　ＧＰＳ受信機能（第２通信手段）

４００　認証サーバ（第２情報処理装置）

４１１～４１３　ファイルサーバ（特定の位置に固定された端末）

５０１～５０３　ＧＰＳ衛星

６００　認証サーバが持つ情報テーブル

６０１～６０３　情報テーブルの各アクセス許可領域の行

１　無線ＬＡＮアクセスポイント

２０　無線ＬＡＮアクセスポイントの通信可能範囲

２１　ロックＣＤ売り場（領域）

２２　ジャズＣＤ売り場（領域）

３　携帯電話

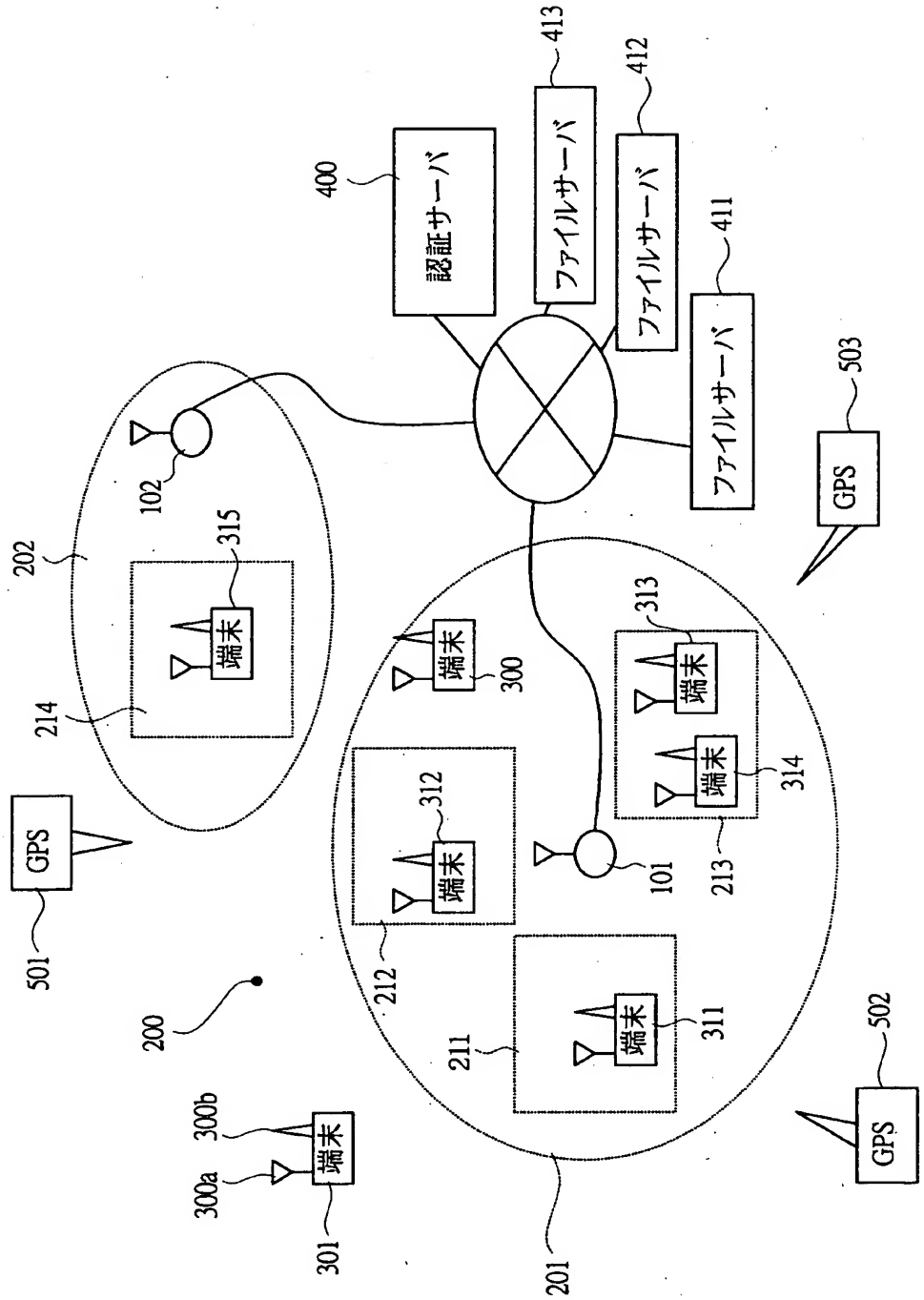
４０　認証サーバ

４１　ファイルサーバ

【書類名】　図面

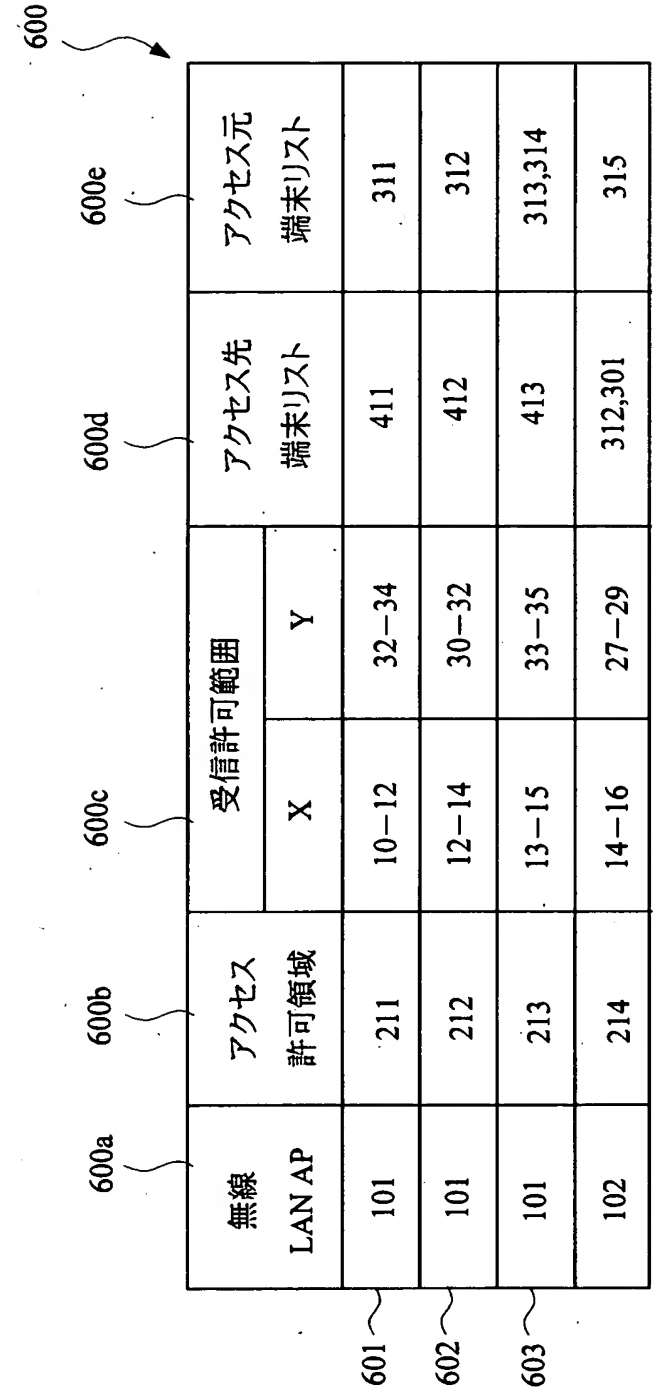
【図１】

図 1


認証サーバ
400
ファイルサーバ
413
ファイルサーバ
412
ファイルサーバ
411
GPS
503
GPS
502
GPS
501
102
101
202
214
315
端末
300
313
314
312
213
212
211
311
200
300b
300a
301
201

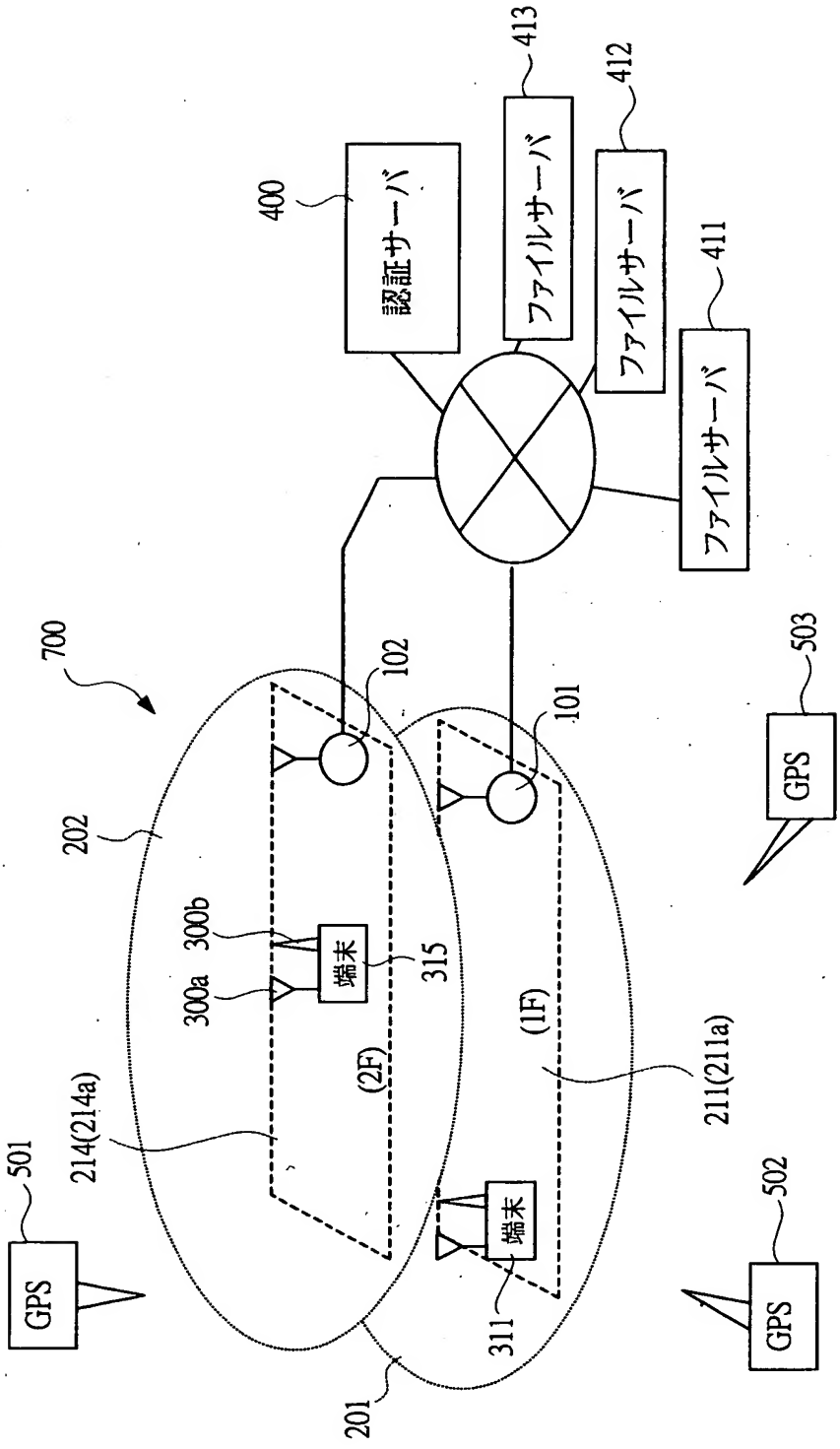
【図２】

図 2


600
600a
600b
600c
600d
600e
無線 LAN AP
アクセス許可領域
受信許可範囲
X
Y
アクセス先端末リスト
アクセス元端末リスト
101 211 10−12 32−34 411 311
101 212 12−14 30−32 412 312
101 213 13−15 33−35 413 313,314
102 214 14−16 27−29 312,301 315
601
602
603

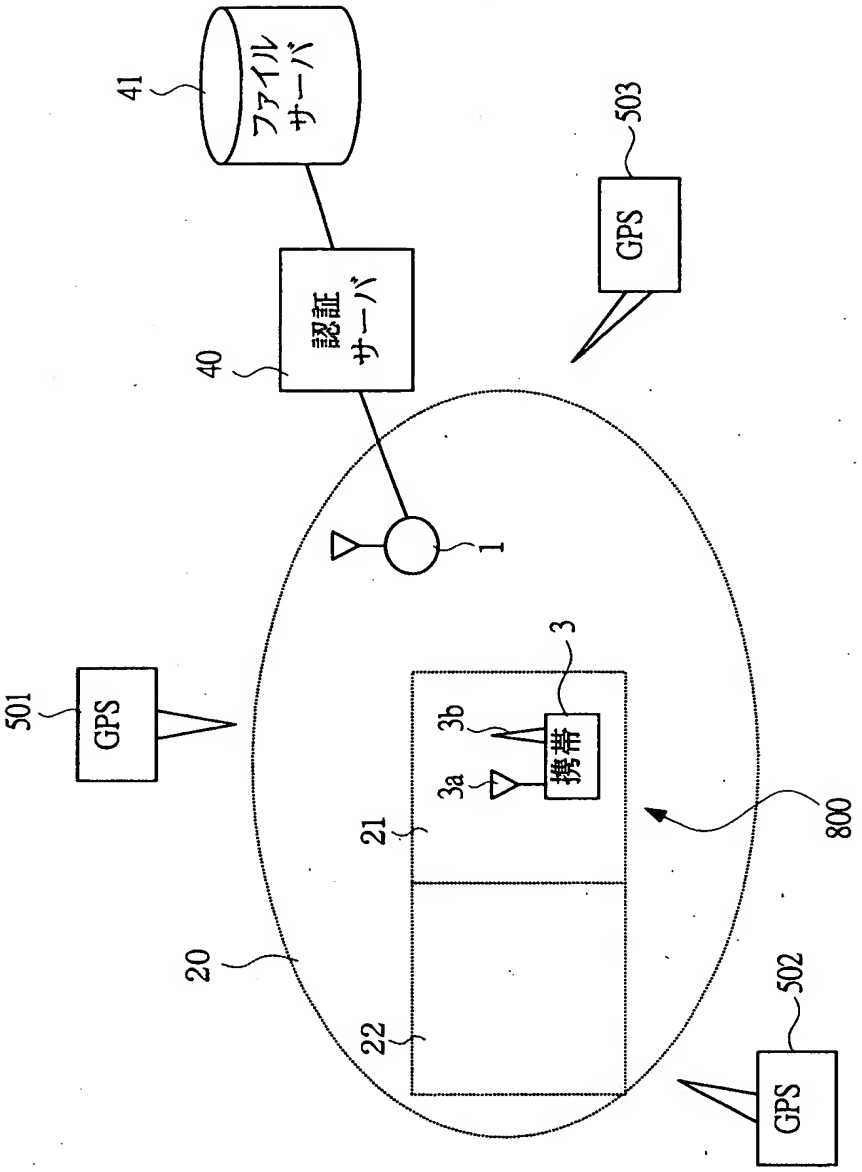
【図３】

図 3


700
400
認証サーバ
413
ファイルサーバ
412
ファイルサーバ
411
ファイルサーバ
102
101
202
201
300b
300a
端末
315
311
端末
(2F)
(1F)
214(214a)
211(211a)
501
GPS
502
GPS
503
GPS

【図４】

図４


ファイル
サーバ
41
503
GPS
認証
サーバ
40
1
3
3b
携帯
3a
501
GPS
21
800
20
22
502
GPS

【図５】

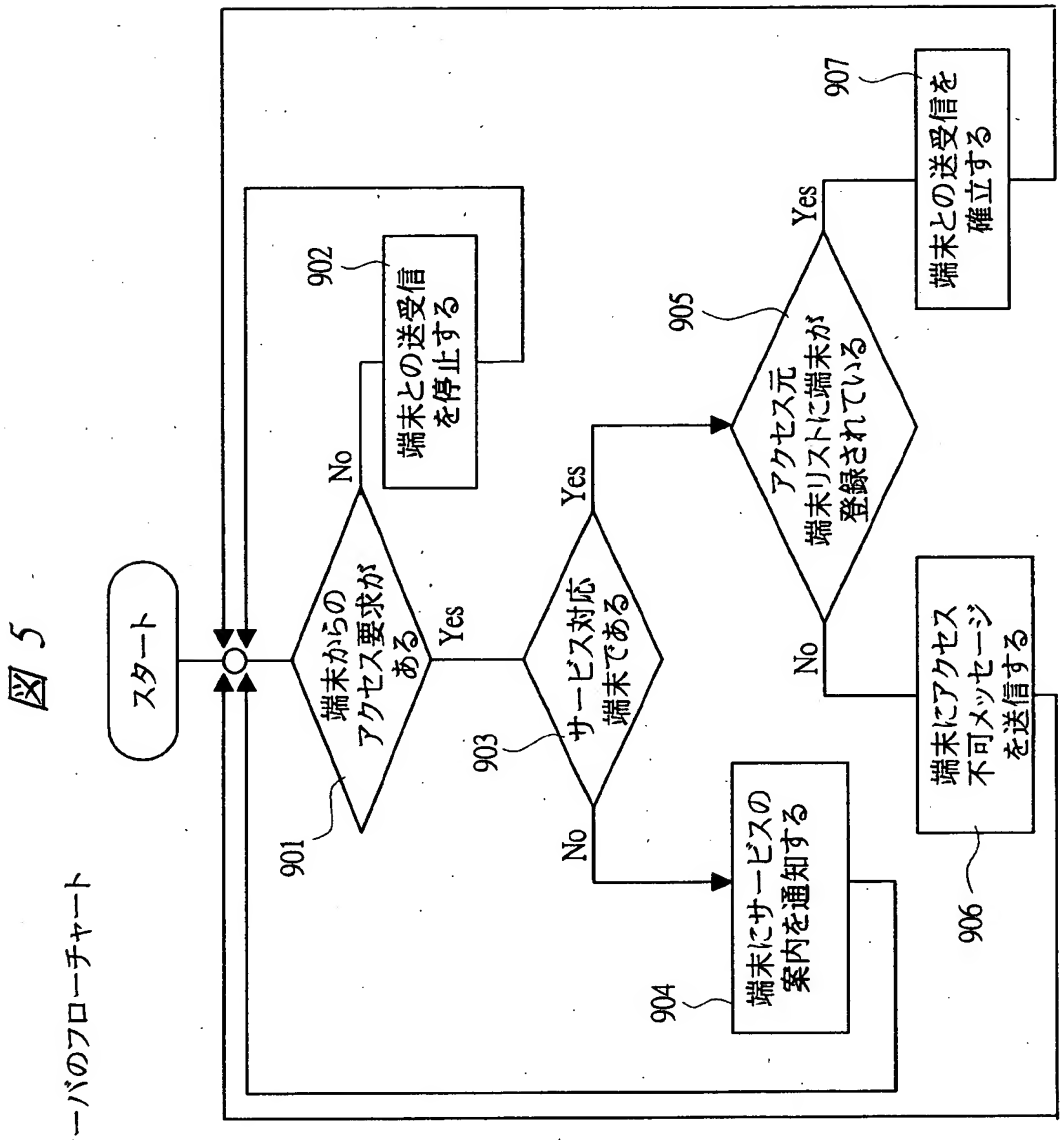


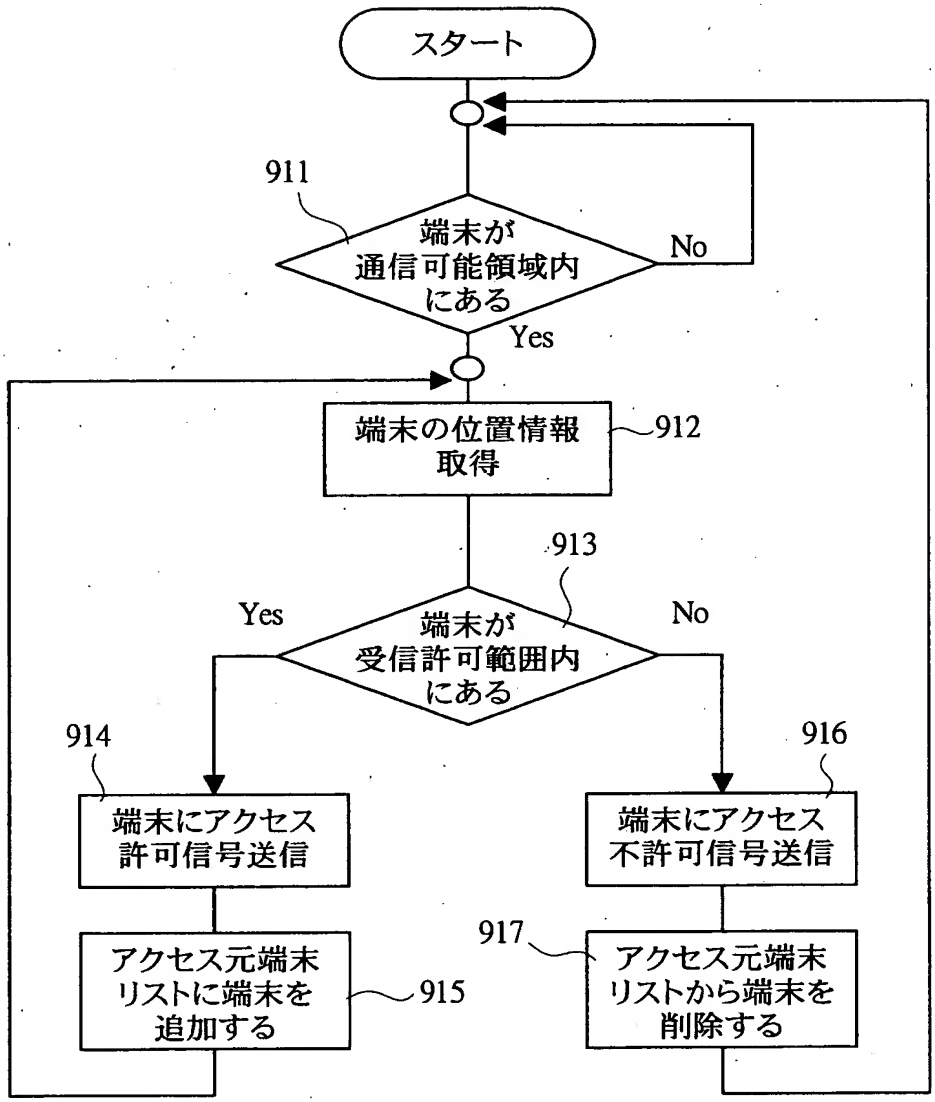
図５

ファイルサーバのフローチャート

【図６】

図 6

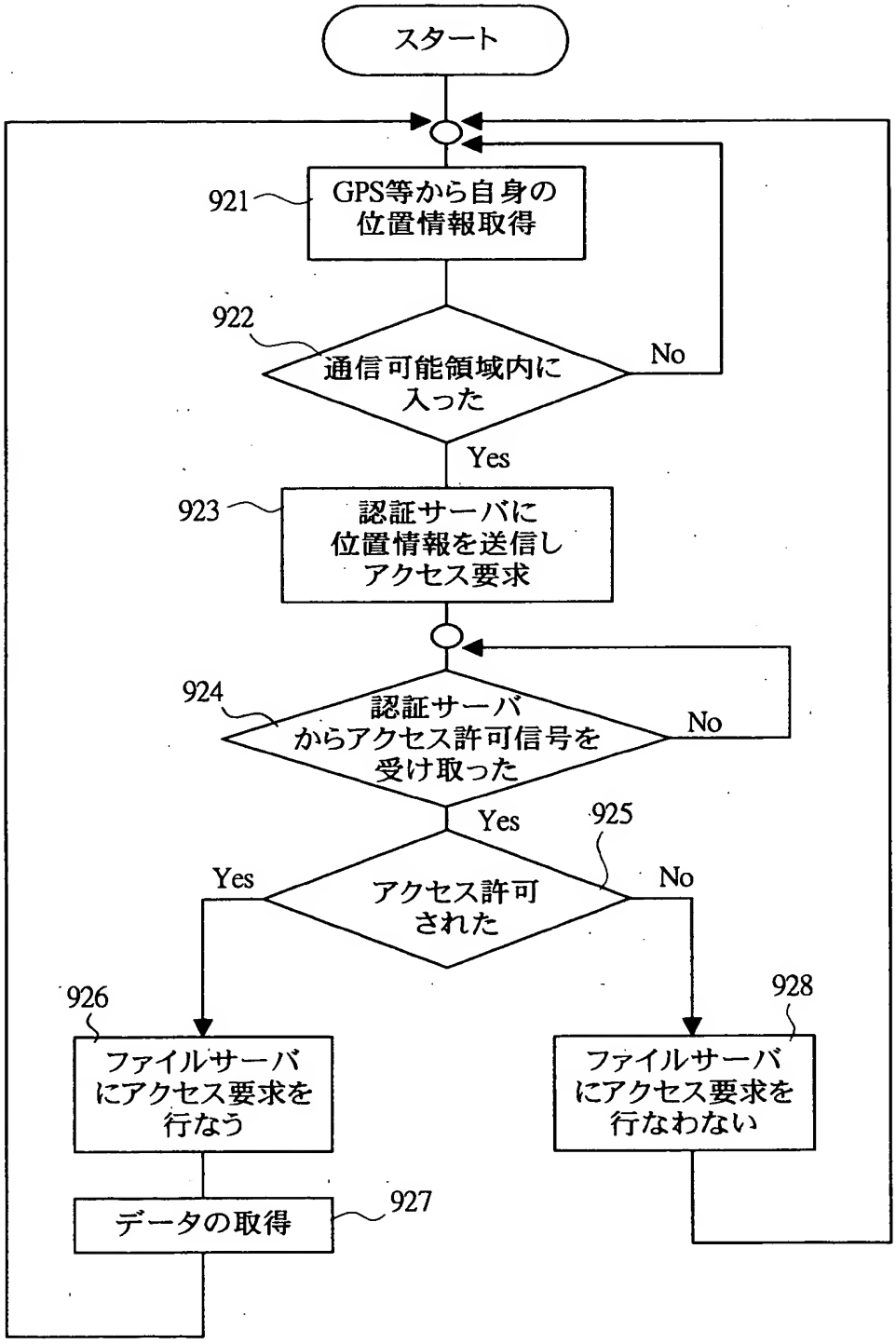
認証サーバのフローチャート



【図７】

図 7

端末のフローチャート



【書類名】　要約書

【要約】

【課題】　無線ネットワーク上の情報資源に対するアクセス可能範囲を限定することで、不正アクセスの防止や的確な情報伝達を可能とする。

【解決手段】　端末３１１やファイルサーバ４１１～４１３は、複数のＧＰＳ衛星５０１～５０３から受信した物理的な距離、複数の携帯電話基地局から受信した物理的な距離等の自身の現在位置情報と、無線ＬＡＮネットワークのセグメント（アクセスポイント）情報等の位置情報を認証サーバ４００へ送信する。認証サーバ４００はその位置情報の正当性を判断し、ネットワーク上のファイル等の情報資源へのアクセスを制御する。ネットワーク上のファイル装置に対するアクセス可能範囲を限定することで、自由に移動可能な端末に対して、不正アクセスの防止や的確な情報伝達が可能となる。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所